IN THE CLAIMS:

1. (Currently Amended) A method for increasing security of a mobile terminal that has been lost, stolen, or misplaced by a user, comprising:

receiving a guard message at the mobile terminal,

authenticating the guard message,

locking at least one communication capability of the mobile terminal, and

securing at least some data that is stored in the mobile terminal,

wherein initiation of the method requires inputting a personal identification code at a location separate from the mobile ~~terminal.~~ terminal, and

wherein the step of securing the stored data includes destroying at least part of the stored data after uploading the at least part of the stored data from the mobile terminal.

2. (Original) The method of claim 1, wherein the guard message employs a smart message implemented as a bearer-independent object, or employs wireless access protocol push messaging.

3. (Original) The method of claim 1, wherein the guard message employs synchronization markup language device management.

4. (Currently Amended) A method for increasing security of a mobile terminal that has been lost, stolen, or misplaced by a user, comprising:

receiving a guard message at the mobile terminal,

authenticating the guard message,

locking at least one communication capability of the mobile terminal, and

securing at least some data that is stored in the mobile terminal,

wherein initiation of the method requires inputting a personal identification code at a location separate from the mobile terminal,

wherein the step of securing the stored data includes destroying at least part of the stored data after uploading the at least part of the stored data from the mobile terminal, and

~~The method of claim 1,~~ wherein the guard message employs synchronization markup language device management if another program of the mobile terminal employs synchronization markup language device management, and otherwise the guard message either employs a smart message implemented as a bearer-independent object or employs wireless access protocol push messaging.

5. (Original) The method of claim 1, wherein the personal identification code is different from a code used to operate the mobile terminal, and wherein initiation of the method also requires inputting a mobile terminal identifier.

6. (Original) The method of claim 5, wherein the personal identification code and the code used to operate the mobile terminal are both user-selected.

7. (Original) The method of claim 1, wherein the user provides the personal identification code to an attendant, and the attendant then sends the guard message.

8. (Original) The method of claim 1, wherein the guard message is sent repeatedly until an acknowledgment is received, or is sent when the mobile terminal is detected to be connected to a network, or both.

9. (Original) The method of claim 8, wherein the acknowledgment includes information about where the mobile terminal is located.

10. (Currently Amended) The method of claim 1, ~~wherein the step of securing the stored data includes destroying at least part of the stored data.~~ wherein at least some of the stored data is encrypted prior to the uploading, after the receiving of the guard message.

11. CANCEL

12. (Original) A computer readable medium encoded with a software data structure sufficient for performing the method of claim 1.

13. (Currently Amended) A mobile terminal for increasing security in the event of loss, theft, or misplacement by a user, comprising:

a transceiver for receiving a guard message;

an authentication unit for authenticating the guard message and providing an authentication signal;

a communication locking mechanism, responsive to the authentication signal, for securing at least one communication capability of the mobile terminal; and

a data securing mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal,

wherein the guard message is transmitted to the transceiver when the user inputs a personal identification code at a location separate from the mobile ~~terminal.~~ terminal, and

wherein the data securing mechanism is also for destroying at least part of the stored data after uploading at least part of the stored data from the mobile terminal.

14. (Original) The mobile terminal of claim 13, wherein the guard message employs a smart message implemented as a bearer-independent object, or employs wireless access protocol push messaging.

15. (Original) The mobile terminal of claim 13, wherein the guard message employs synchronization markup language device management.

16. (Currently Amended) A mobile terminal for increasing security in the event of loss, theft, or misplacement by a user, comprising:

a transceiver for receiving a guard message;

an authentication unit for authenticating the guard message and providing an authentication signal;

a communication locking mechanism, responsive to the authentication signal, for securing at least one communication capability of the mobile terminal; and

a data securing mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal,

wherein the guard message is transmitted to the transceiver when the user inputs a personal identification code at a location separate from the mobile terminal,

wherein the data securing mechanism is also for destroying at least part of the storeddata after uploading at least part of the stored data from the mobile terminal, and

~~The mobile terminal of claim 13,~~ wherein the guard message employs synchronization markup language device management if another program of the mobile terminal employs synchronization markup language device management, and otherwise the guard message either employs a smart message implemented as a bearer-independent object or employs wireless access protocol push messaging.

17. (Original) The mobile terminal of claim 13, wherein the personal identification code is different from a code used to operate the mobile terminal, and wherein transmission of the guard message also requires inputting a mobile terminal identifier.

18. (Original) The mobile terminal of claim 17, wherein the personal identification code and the code used to operate the mobile terminal are both user-selected.

19. (Original) The mobile terminal of claim 13, wherein the guard message is received from an attendant, in response to the attendant obtaining the personal identification code from the user.

20. (Original) The mobile terminal of claim 13, wherein the guard message is sent repeatedly to the transceiver until an acknowledgment is received from the transceiver, or is sent when the mobile terminal is detected to be connected to a network, or both.

21. (Original) The mobile terminal of claim 20, wherein the acknowledgment includes information about where the mobile terminal is located.

22. CANCEL

23. CANCEL

24. (Original) The mobile terminal of claim 13, further comprising an emergency power supply for at least powering the communication locking mechanism and the data securing mechanism if normal power to the mobile terminal is disabled.

25. (Currently Amended) The mobile terminal of claim [[23]] 13, wherein the uploading is encrypted.